

PX 689

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

GBM Global Holding Company Limited

Plaintiff,

v.

The Unidentified Individuals Listed on
Schedule A,

Defendants

Case No. 1:21-cv-06284

**DECLARATION OF DAISY LU LI IN
SUPPORT OF PETITION FOR
TEMPORARY RESTRAINING ORDER IN
AID OF ARBITRATION**

I, **DAISY LU LI** declare as follows:

1. I am the Chief Compliance Officer of GBM Global Holding Company Limited (the “**Company**”) which is the Plaintiff in the captioned matter. This declaration is based on my personal knowledge of the facts stated herein or on business records that were made at the time in the regular course of business. If called as a witness, I could and would testify to the statements made herein.

2. The Company is the owner of BitMart, a cryptocurrency exchange established in 2018 (<https://www.bitmart.com/>). The Company is the parent of Bachi.Tech Corporation (“**Bachi**”), a subsidiary that operates the BitMart cryptocurrency exchange. Bachi is incorporated in New Jersey. Bachi runs its operations and has employees in both New York and New Jersey.

3. As a cryptocurrency exchange, over 400 cryptocurrencies are traded on BitMart. The Bitcoin Satoshi Vision (“**BSV**”) token is one of them. An overview of blockchain technology and BSV specifically has been set out more fully in the accompanying declaration of the Company’s technical lead, Wei Li.

4. Created in 2018, the BSV token is a cryptocurrency that is generated by forking the Bitcoin Cash blockchain (which is itself a fork of Bitcoin) and adjusting the blockchain protocol by using blocks that are larger, which in turn helps to reduce transaction fees. Bitcoin Association, a non-profit association in Switzerland, is the organization that supports the BSV blockchain network and provides infrastructural tools such as the BSV node software which is needed to access the BSV blockchain network.

5. On July 8, 2021, Bitcoin Association announced that it has been made aware of an illegal attack by a malicious actor that has recently been carrying out block re-organisation attacks on the BSV network. Bitcoin Association reported that the hack resulted in malicious double spending of fake BSV tokens.

6. At the time, the Company was not aware of Bitcoin Association's announcement and the deposit/trading/withdrawal functions of BSV on BitMart were working as normal. The Company only came to know of Bitcoin Association's announcement on July 10, 2021.

7. On July 9, 2021, the BitMart exchange experienced a malicious hack between 2:30 pm to 10:00 pm. In that window, the hacker(s) registered 92 user accounts with BitMart and manipulated them to carry out trades using fake BSV tokens which the hacker(s) generated through a "51% attack" of the BSV network. *See* Accompanying Wen Li Declaration.

8. The hacker(s) initiated deposits of BSV tokens mined on the private chain to the 92 user accounts they opened on BitMart. These deposits went undetected by BitMart as BitMart's verification system only verified these tokens against the hackers' fraudulent records on the fake BSV blockchain the hackers created during the 51% attack. As such, the hacker(s) managed to get BitMart to confirm these BSV tokens as proper deposits. A total of 91,000 BSV tokens were deposited into the digital wallets linked with the 92 BitMart accounts that the hacker(s) opened.

9. Once BitMart confirmed these deposits, the hackers immediately began using the deposited BSVs to trade for other cryptocurrencies on the exchange before withdrawing these cryptocurrencies from the exchange to other exchanges. A total of 91,000 BSV tokens mined from the hackers' private chain were deposited and used to procure other cryptocurrencies on the BitMart exchange that were worth approximately US \$6.07 million:

Cryptocurrency (Trading Symbol)	Number of Coins/Tokens
Bitcoin (BTC)	11.106
Ethereum (ETH)	216.523
Litecoin (LTC)	668.196
Cardano (ADA)	130,780.8
USDC (ERC-20)	605,336
USD Coin (USDC)	283,984.407
Polygon (MATIC)	297,691
Stellar (XLM)	969,308.31
Holo (HOT)	29,912,899
XRP (XRP)	3,994,932.49

10. The Company only came to know of the hackers' suspect trading activities at about 10 pm on July 9, 2021. Very quickly, the Company identified the 92 accounts that were affected and froze them. Thereafter, BitMart investigated its records showing the cryptocurrencies that the hackers cashed out on and transferred to other crypto exchanges. So far, the Company has discovered that the some of the cryptocurrencies were transferred to the following crypto exchanges:

Cryptocurrency Exchange	Entity that owns the Cryptocurrency Exchange	Number of Coins/Tokens
Binance	Binance Holdings Limited	At least 2 BTC and 21611,9 XRP.
Huobi	Huobi Global Limited	At least 969,784.13 XRP.
OKex	OKEX MALTA LTD	At least 24664.99 USDT.
Kucoin	Mek Global Limited	The number of cryptocurrencies being held is unknown, but transfers to this exchange are confirmed

Cryptocurrency Exchange	Entity that owns the Cryptocurrency Exchange	Number of Coins/Tokens
Hitbtc	Hit Tech Solutions Development Ltd	The number of cryptocurrencies being held is unknown, but transfers to this exchange are confirmed
Nicehash	Nicehash Ltd	At least 135,217 XRP.
BW.com	Collinstar Holding Pty. Ltd.	The number of cryptocurrencies being held is unknown, but transfers to this exchange are confirmed.
Ascendex	BMXDM Technology Pte. Ltd.	At least 500 XRP.

11. BitMart has suffered losses worth about \$5.27 million having refunded the cryptocurrencies to its users who transacted with the hackers using their legitimate cryptocurrencies. BitMart did so to maintain its commercial relationship with its clients and to uphold its reputation. It must now seeks to recover these losses from the hackers who caused them. Investigations are ongoing and BitMart has reported this attack to the FBI. The Company will shortly be commencing arbitration against the hackers.

12. Meanwhile, we have reached out to the other crypto exchanges where the cryptocurrencies were transferred to and requested a freeze of the affected accounts. Some of them have agreed to a temporary freeze out of goodwill. However, these exchanges have also informed us that they need a court order against the Defendants to maintain the freeze, otherwise they would have no choice but to release the accounts. As such, time is of the essence and the Company has authorized its attorneys in the U.S. to move for a temporary restraining order.

13. The Company is also submitting these moving papers under seal because it needs to prevent the hackers from learning of this legal action lest they further transfer or dissipate the cryptocurrencies before all possible injunctive relief is effectuated. These moving papers also set out BitMart's intellectual property and trade secrets, including, among others things, its policies for confirming validated blockchains.

14. We have identified at least two New York-resident users of our exchange who were victimized and refunded by us in the course of this BSV hack. We have identified a total of 42-U.S.-based users who were victims of this same hack.

I declare under penalty of perjury that the foregoing is true and accurate to the best of my knowledge, information, and belief.

Signed July 23, 2021.

/s/ Daisy Lu Li

Daisy Lu Li
Fort Lee, New Jersey